



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/579,801	05/15/2006	Yong Ding	25515-0002	3452
29052	7590	07/26/2007	EXAMINER	
SUTHERLAND ASBILL & BRENNAN LLP			LE, CANH	
999 PEACHTREE STREET, N.E.				
ATLANTA, GA 30309				
			ART UNIT	PAPER NUMBER
			2139	
			MAIL DATE	DELIVERY MODE
			07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

SJD

Office Action Summary	Application No.	Applicant(s)
	10/579,801	DING ET AL.
	Examiner	Art Unit
	Canh Le	2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 15 May 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-16 is/are rejected.
- 7) Claim(s) 4,11 and 13-16 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 15 May 2006 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>5/15/2006</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This Office Action is in response to the application filed on 5/15/2006. Claims 1-16 are pending and have been examined.

Specification

The abstract of the disclosure is objected to because the abstraction exceeds more than 150 words in length. Correction is required. See MPEP § 608.01(b).

The disclosure is objected to because of the following informalities: There are some abbreviations that do not spell out the expression the first time it is used. An abbreviation should spell out the expression the first time it is used and then be followed by parentheses. Some abbreviations can be found in specification such as SSS in paragraph [0028] and BCDA in paragraph [0038]. Appropriate correction is required.

Claim Objections

Claims 4, 11, and 13-16 are objected to because of the following informalities:

Claim 4 recites "the range of 20~30" should be "the range of 20~28" based on TABLE 2 of the specification. Appropriate correction is required.

Claims 11 and 13-16 are objected with the same reason above.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-2 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the left group", "the number", "the upper bound", "the length", "Step1: the signatory (S)", " Step3 .. the generated random braid", "the signature of message (M)". There are insufficient antecedent bases for these limitations in the claim.

Claim 2 recites the limitation "the left canonical form" in step 1b. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4 and 13-14 are rejected under 35 U.S.C. 102(b) as being anticipated by K.H. Ko et al., "New Signature Scheme Using Conjugacy Problem", November 11, 2002, pages 1-13.

As per claim 1:

Art Unit: 2139

Ko teaches a digital signature scheme based on braid group conjugacy problem, parameters involved in this scheme comprising a signatory S, a signature verifying party V, a message M needing signature, an integer n for the number of generators in the braid group, an integer m for the number of generators in the left subgroup, an integer l for the upper bound of the length of a braid, a braid group B.sub.n(l), a left subgroup LB.sub.m(l) of B.sub.n(l), a right subgroup RB.sub.n-1-m(l) of B.sub.n(l), a one way hash function h from bit sequence {0,1}* to braid groups B.sub.n(l); said signature scheme comprising the following steps of:

- (a) Step 1. the signatory (S) selecting three braids $x.\epsilon.LB.sub.m(l)$, $x'.\epsilon.B.sub.n(l)$, $a.\epsilon.B.sub.n(l)$, and making them meet $x'=a.sup.-1xa$, moreover, with known x and x' , it being impossible to find a in calculation, and considering braid pair(x',x) as a public key of signatory (S), braid a as a private key of signatory (S) [pg. 4-5; section 2.3 Description of conjugacy signature scheme section; "Key generation ...on the braid groups"];
- (b) Step 2. signatory (S) using hash function h for message (M) needing signature to get $y=h(M).\epsilon.B.sub.n(l)$ [pg. 4-5; section 2.3 Description of conjugacy signature scheme section; "Signing: Given a message m, a signature ... on the braid groups"];
- (c) Step 3. generating a braid $b.\epsilon.RB.sub.n-1-m(l)$ at random, then signing the message (M) with the own private key a and the generated random braid b to obtain $Sign(M)=a.sup.-1byb.sup.-1a$; and Step 4. the signatory (S) outputting message (M) and

the signature of message (M) $\text{Sign}(M)$ [pg. 4-5; section 2.3 Description of conjugacy signature scheme section].

As per claim 2:

Ko further teaches the digital signature scheme based on braid group conjugacy problem according to claim 1, wherein generating the public key braid pair (x', x) and the private key braid a of signatory (S) in said step 1 comprises the following steps of:

(a) Step 1a. selecting a distance d between system parameter braid groups public key pairs [pg. 9-10; 4.1 Random braids and braid signature scheme; “the distance $d(x,y)$ between x and y is defined by ... Return accept if and only if”].

(b) Step 1b. representing x into the left canonical form
 $x=.\text{DELTA}..sup.u.pi..sub.1.pi..sub.2 \dots .pi..sub.1$ [pg. 5-6; 3.1 Brief introduction to braid group section; “We introduce necessary ...This unique decomposition of a braid b is called a left canonical form...in a high probability”];

(c) Step 1c. selecting a braid b at random to belong to a set $B_{\text{sub}}(5 l)$ [pg. 5-6; 3.1 Brief introduction to braid group section; pg. 9-10; 4.1 Random braids and braid signature scheme section ; “We first choose b belong to set $B_n(5 l)$ if $l(x)=l$... Return accept if and only if”];

(d) Step 1d. calculating $x.sup.'=sup.-1.sup.xb,a=b$ [pg. 6-7; 3.2 Conjugator search problem in Braid groups section; pg. 9-10; 4.1 Random braids and braid signature scheme section ; “We first choose b belong to set $B_n(5 l)$ if $l(x)=l$. Then

we apply a random sequence of cyclings and decyclings to ...Return accept if and only if';

(e) Step 1e. generating a bit at random, if 1, calculating $x.sup.'=decycling(x.sup.)$, $a=a.pi..sub.1$; if not 1, calculating $x.sup.'=cycling(x.sup.)$, $a=a.tau..sup.u(.pi..sub.1)$ [pg. 6-7; 3.2 Conjugator search problem in Braid groups section; “There are two useful conjugations of a braid ...The cycling on x is given by ... and the decycling on x ... level for MCSP as well”; pg. 9-10; 4.1 Random braids and braid signature scheme section ; “We first choose b belong to set $Bn(5 l)$ if $l(x)=l$. Then we apply a random sequence of cyclings and decyclings to ...Return accept if and only if’];

(f) Step 1f. judging whether $x.sup.'$ belongs to $SSS(x)$ and whether $l(x.sup.).ltoreq.d$, if all the conditions are yes, outputting the braid pair($x, x.sup.$) as the public key, a as the private key; if either of them is not, performing step 1e [pg. 6-7; 3.2 Conjugator search problem in Braid groups section; “Super Summit Set We now discuss a mathematical solution The super summit set $SSS(x)$ of s is defined byThere are two useful conjugations of a braidThe cycling on x is given by and the decycling on x ... level for MCSP as well”; pg. 9-10 Random braids and braid signature scheme section].

As per claim 3:

Ko further teaches the digital signature scheme based on braid group conjugacy problem according to claim 1, wherein the process for obtaining

y=h(M).epsilon.B.sub.n(l) by using the hash function h in said step 2 comprises the following steps of:

- (a) Step 2a, selecting an ordinary hash function H, with a length of output H(M) is l [log(2,n!)], then dividing H(M) into l sections R.sub.1.parallel.R.sub.2.parallel. . . parallel.R.sub.1 in equal at one time **[pg. 9-10; 4.1 Random braids and braid signature scheme section]**.
- (b) Step 2b, corresponding Ri to a permutation braid Ai, then calculating h(M)=A1*A2 . . . Al, that is the h(M) required **[pg. 9; 4.1 Random braids and braid signature scheme section]**.

As per claim 4:

Ko further teaches the digital signature scheme based on braid group conjugacy problem according to claim 1, wherein a integer n for the number of generators in a braid group is in the range of 20.about.30, an upper value of the braid length is l=3, d=4, and an left subgroup n-m=4 **[pg. 11-12; 4.3 Parameters suggestion and performance section; 4.4 Performance table section]**.

As per claim 13:

Claim 13 is essentially the same as claim 4 and rejected under the same reasons as applied above.

As per claim 14:

Claim 14 is essentially the same as claim 4 and rejected under the same reasons as applied above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 5-12 and 15-16 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over K.H. Ko et al., "New Signature Scheme Using Conjugacy Problem", November 11, 2002, pages 1-13.

As per claim 5:

Ko teaches a verifying method based on braid group conjugacy digital signature scheme, comprising the following steps of:

- (a) Step 1. a signature verifying party (V) obtaining a public key of a signatory (S) after receiving a message (M) and its signature $\text{Sign}(M)$ transmitted from the signatory (S) [pg. 4-5, 2.3 Description of conjugacy signature scheme section];
- (b) Step 2. calculating the message M by employing a system parameter hash function h , and obtaining $y=h(M)$ [pg. 4, 2.3 Description of conjugacy signature scheme; " Signing: Given a message m , ... for $y = h(m)$ "];

(c) Step 3. judging whether sign(M) and y are conjugate or not, if not, sign(M) is an illegal signature, and the verification fails; if yes, perform step 4 [pg. 4-5; 2.3

Description of conjugacy signature scheme; “Verifying: A signature ...implement it on the braid groups”; pg. 7; 3.3 Conjugacy decision algorithm in braid group (BCDA) to pg. 10; “Verifying Algorithm: Ver (pk,m,sigma) = {accept|reject}”]; and

(d) Step 4. calculating sign(M) x' and xy by using the public key of obtained S, and judging whether they are conjugate or not, if not, sign(M) is an illegal signature, the verification fails; if yes, sign(M) is the legal signature of message (M) [pg. 4-5; 2.3

Description of conjugacy signature scheme; “Verifying: A signature ...implement it on the braid groups”; pg. 7; 3.3 Conjugacy decision algorithm in braid group (BCDA) to pg. 10; “Verifying Algorithm: Ver (pk,m,sigma) = {accept|reject}”].

As per claim 6:

Ko further teaches the verifying method based on braid group conjugacy digital signature scheme according to claim 5, wherein the form of obtaining the public key of signatory (S) in step 1 is an out-band form or a form of receiving the public key transmitted from signatory (S) [pg. 4-5; 2.3 Description of conjugacy signature scheme; “Key generation: A public key is a CSP-hard pair ... implement it on the braid groups”].

As per claim 7:

Ko further teaches the verifying method based on braid group conjugacy digital signature scheme according to claim 5, wherein algorithm BCDA is employed in judging whether $\text{sign}(M)$ and y are conjugate or not in step 3 and judging whether $\text{sign}(M) x'$ and xy are conjugate or not in step 4 [pg. 7-8; **3.3 Conjugacy decision algorithm in braid groups (BCDA) section**].

As per claim 8:

Claim 8 is essentially the same as claims 1 and 5 and rejected under the same reasons as applied above.

As per claim 9:

Claim 9 is essentially the same as claim 2 and rejected under the same reasons as applied above.

As per claim 10:

Claim 10 is essentially the same as claim 3 and rejected under the same reasons as applied above.

As per claim 11:

Claim 10 is essentially the same as claim 4 and rejected under the same reasons as applied above.

As per claim 12:

Claim 12 is essentially the same as claim 7 and rejected under the same reasons as applied above.

As per claim 15:

Claim 15 is essentially the same as claim 4 and rejected under the same reasons as applied above.

As per claim 16:

Claim 16 is essentially the same as claim 4 and rejected under the same reasons as applied above.

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

US 2002/0001382 A1 to ANSHEL et al.

US 2004/0240672 A1 to Girault et al.

US 7,133,523 B2 to Campagna et al.

Ki Hyoung Ko, Doo Ho Choi, Mi Sung Cho, and Jang Won Lee, "New Signature Scheme Using Conjugacy Problem", pp. 1-13, November 11, 2002.

Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park, "New public-Key Crystosystem Using Braid Groups", CRYPTO 2000, LNCS 1880, pp. 166-183, 2000.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Art Unit: 2139

Customer Service Representative or access to the automated information system, call
800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le

July 18, 2007


CHRISTIAN LE
AU 2139